Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Dr. Kpatcha Bayarou
Rheinstraße 75
64295 Darmstadt
Germany

Phone +49 6151 869-274
Fax +49 6151 869-224
kpatcha.bayarou@sit.fraunhofer.de
www.sit.fraunhofer.de

AUTOSEC

AUTOMATED NETWORK SECURITY FOR SDN AND CONNECTED CLIENTS

Software-Defined Networking (SDN) provides new opportunities to manage networks in a simplified and efficient manner with the help of a centralized network controller. Increase in flexibility and reduction in cost have already motivated many enterprises to move towards adopting SDN. Making use of the unique features of SDN, Fraunhofer SIT has developed AutoSec, a solution to integrate novel protection features into SDN-based networks and the devices connected to them.

Software-Defined Networking (SDN) & Network Functions Virtualization (NFV)

The concept of SDN is based on the separation of the control plane from the data plane: An SDN controller (representing the control plane) makes decisions based on forwarding rules. Routers, switches, etc. (representing the data plane) forward the data accordingly. These two planes communicate using protocols such as OpenFlow. Additionally, NFV allows manufacturers of SDN network components to provide their customers with a unified configuration management and a programmable centralized control of the overall network.

Client Integration

AutoSec integrates the clients (such as workstations or laptops) into SDN and NFV by making their configuration programmable. In case of a security threat observed by a network monitor, AutoSec is able to dynamically apply security rules to execute actions that help to resolve the incident. For example, when a computer worm is spreading inside an enterprise network, AutoSec is able to instruct the network components to hinder the worm from replication and to quarantine the infected clients. Then, AutoSec reconfigures non-infected clients to immunize against the worm.

Dynamic Security

AutoSec employs system configuration management tools to integrate connected devices into the network protection strategies. Depending on the respective threat situations given in a network, AutoSec is able to enable the following security capabilities dynamically:

- Encryption and integrity protection of network connections
- Activate or change firewall rules
- Deploy malware detection and removal tools
- Running additional network monitoring tools to gain detailed attack information
- Customized device and service remote configuration

Further features can be defined and imposed by the device and network operators.

AutoSec is currently in a Proof of Concept stage. Fraunhofer SIT offers SDN and data center operators, ISPs, configuration management tool providers, and telecoms to integrate AutoSec capabilities into their products, networks, and services.